AMENDMENTS TO THE CLAIMS:

This listing of the claims will replace all prior versions, and listings, of the claims in this application.

Listing of Claims:

1. (Original) A cryptographic system (1) comprising

first cryptographic algorithm means (2) for enabling cryptographic operations, input/output means (3, 4) for receiving input streams and sending output streams wherein said input streams are transformed to said output streams by said cryptographic operations,

at least one test plaintext P_i and for each test plaintext P_i a corresponding test ciphertext C_i,

receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i ,

checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (2) when using said apoptosis key K_i,

switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm means (2), wherein said stopping by said switching means (7) is triggered by said checking means (6).

2. (Original) System as claimed in claim 1, wherein said cryptographic system (1) includes at least one second cryptographic algorithm means (8) wherein said switching means (7) enables switching to said at least one second cryptographic algorithm means (8).

3. (Original) System as claimed in claim 1, wherein

said receiving means (5) is made for accepting control streams which include at least one plaintext P_i, for each plaintext P_i a corresponding ciphertext C_i and a corresponding apoptosis key

K_i and

said checking means (6) is made for trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i, wherein said checking is done with said apoptosis key of said equal test plaintext P_i and said equal test ciphertext C_i .

4. (Original) System as claimed in claim 1 further comprising a cascaded list of different cryptographic algorithm means.

5. (Original) A method for creating a cryptographic system (1) for carrying out cryptographic operations characterized by the steps of

implementing within said cryptographic system (1) a first cryptographic algorithm enabling said cryptographic operations,

selecting at least one test plaintext P_i and enciphering each test plaintext P_i with said first cryptographic algorithm and with a corresponding apoptosis key K_i thereby generating a corresponding test ciphertext C_i for each test plaintext P_i ,

implementing within said cryptographic system (1) said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i

implementing within said cryptographic system (1) receiving means (5) for receiving a control stream which is including at least one apoptosis key K_i ,

implementing within said cryptographic system (1) checking means (6) for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i,

implementing within said cryptographic system (1) switching means (7) for stopping said cryptographic operations with said first cryptographic algorithm, wherein said stopping by said switching means (7) is triggered by said checking means (6).

6. (Original) Method as claimed in claim 5, further comprising the step of

implementing within said cryptographic system (1) at least one second cryptographic algorithm for said ciphering operations, and switching by said switching means (7) to said at least one second cryptographic algorithm.

7. (Original) Method as claimed in claim 5, further comprising the step of publishing said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i.

8. (Original) A method for operating a cryptographic system (1) for carrying out cryptographic operations characterized by the steps of

providing a first cryptographic algorithm for enabling said cryptographic operations, receiving input streams and sending output streams wherein said input streams are transformed to said output streams by said cryptographic operations, receiving a control stream which is including at least one apoptosis key K_i, checking whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i, stopping said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i.

9. (Previously Presented) Method as claimed in claim 8, further comprising the step of switching to one of a plurality of second cryptographic algorithms for said cryptographic operations after said stopping.

10. (Currently Amended) Method as claimed in claim 8, wherein said receiving of a control stream includes for each apoptosis key K_i receiving of a plaintext P_i and a corresponding ciphertext C_i, and said checking includes trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i, and said received ciphertext C_i, wherein said checking is done with said apoptosis key of said equal test plaintext P_i and said equal test ciphertext C_i.

11. (Original) A computer software product for operating a cryptographic system (1) for carrying out cryptographic operations, said product is characterized by a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, enable the computer to

perform a first cryptographic algorithm that is enabling said cryptographic operations,

receive input streams and send output streams wherein said input streams are transformed to said output streams by said cryptographic operations,

receive a control stream which is including at least one apoptosis key K_i ,

check whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i,

stop said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said apoptosis key K_i.

12. (Previously Presented) Computer software product as claimed in claim 11 ~~10~~, wherein said instructions, when read by a computer, enable the computer to perform at least a second cryptographic algorithm and switch to one of a plurality of second cryptographic algorithms for said cryptographic operations after said stopping.

13. (Original) Computer program comprising program code means for performing the steps of claim 8 when said program is run on a computer.